(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09265254 A**

(43) Date of publication of application: **07 . 10 . 97**

(51) Int. Cl **G09C 1/00**
G09C 1/00
G09C 1/00
G06K 19/00
H04L 9/08
H04L 9/10
H04L 9/32

(21) Application number: **08097410**

(22) Date of filing: **28 . 03 . 96**

(71) Applicant: **DAINIPPON PRINTING CO LTD**

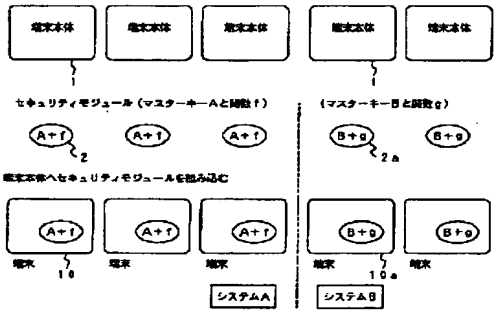
(72) Inventor: **INADA MAYUMI**

(54) MUTUAL AUTHENTICATION SYSTEM FOR INFORMATION RECORDING MEDIUM

(57) Abstract:

PROBLEM TO BE SOLVED: To make a system excellent in security by storing master keys and algorithms needed in operations of mutual authentications by terminals in security modules in readout impossible states to make the keys and the algorithms not to be stolen.

SOLUTION: Same terminal main bodies can be used as terminal main bodies 1 even for systems whose users are different. In security modules 2 to be used in a system A, modules in which master keys As and functions (fs) are used are used and in security modules 2a to be used in a system B, modules in which master keys Bs and functions (gs) are used are used for the common main bodies 1. Then, respective terminals 10, 10b for system A, system B can be constituted by building up security modules different in respective systems in common terminal main bodies. Thus, master keys and algorithms are never abused by being decoded illegally from the outside and the high security of this sysyem is kept.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－265254

(43)公開日　平成９年(1997)10月７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ　1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６３０Ｚ	
		7259－5Ｊ		６３０Ａ	
	６４０	7259－5Ｊ		６４０Ａ	
	６６０	7259－5Ｊ		６６０Ａ	
Ｇ０６Ｋ　19/00			Ｇ０６Ｋ　19/00	Ｔ	

審査請求　未請求　請求項の数６　ＦＤ　（全７頁）　最終頁に続く

(21)出願番号　特願平8－97410

(22)出願日　平成８年(1996)３月28日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　稲田　真弓
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

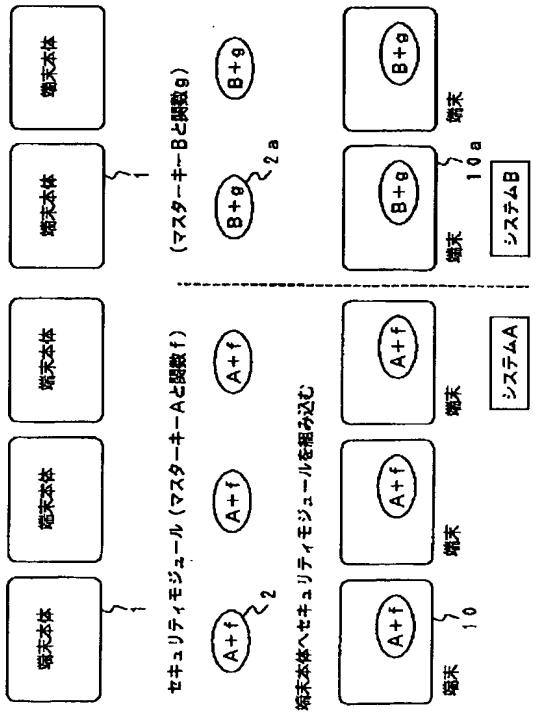
(74)代理人　弁理士　小西　淳美

(54)【発明の名称】　情報記憶媒体の相互認証システム

(57)【要約】

【課題】　端末が相互認証で用いるマスターキー、アルゴリズム等のセキュリティ性を向上し、異なるシステムの端末の製造を容易とする。

【解決手段】　ＩＣメモリを利用した情報記憶媒体と、情報記憶媒体へのアクセスを行う端末とから、少なくとも構成される、情報記憶媒体の相互認証システムにおいて、端末はセキュリティモジュールを備え、端末が使用するマスターキー並びに個別化キー生成アルゴリズム及び認証アルゴリズムを、このセキュリティモジュールに読出不可能な状態で内蔵しておく。セキュリティモジュールは、少なくともマスターキーについては書込可能なメモリを備えたマイクロコンピュータを用いて構成し、ＩＣカード形態とする。



1

【特許請求の範囲】

【請求項１】　ＩＣメモリを利用した情報記憶媒体と、該情報記憶媒体へのアクセスを行う端末とから、少なくとも構成される、情報記憶媒体の相互認証システムにおいて、

端末はセキュリティモジュールを備え、端末が使用するマスターキー、個別化キー生成アルゴリズム及び認証アルゴリズムが、前記セキュリティモジュールに読出不可能な状態で内蔵されている、情報記憶媒体の相互認証システム。

【請求項２】　セキュリティモジュールが、少なくともマスターキーについては書込可能なメモリを備えたマイクロコンピュータで構成されている、請求項１記載の情報記憶媒体の相互認証システム。

【請求項３】　セキュリティモジュールは、個別化キー生成アルゴリズムによって生成するワークキーを、該モジュール内部で使用する、請求項２記載の情報記憶媒体の相互認証システム。

【請求項４】　セキュリティモジュールがＩＣカードである、請求項１～３のいずれか１項に記載の相互認証システム。

【請求項５】　情報記憶媒体がＩＣカードである、請求項１～４のいずれか１項に記載の相互認証システム。

【請求項６】　ＩＣカードがプリペイドＩＣカードである請求項５記載の情報記憶媒体の相互認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＣメモリを利用したＩＣカード等の情報記憶媒体と、それに対してアクセスする端末等とからなるシステムで、相互認証を行うシステムに関する。

【０００２】

【従来の技術】ＩＣメモリを利用し特にＣＰＵを内蔵したＩＣカードはセキュリティ性に優れ、その一つにＣＰＵの演算処理機能等を用いて相互認証が行える点にある。例えば、電話カード等に試みられているプリペイドＩＣカードカードシステムでは、端末に挿入されたカードが正当なものであるか否かを端末は確認し、不正なカードの利用を防ぐことが必要である。一方、カードには金額に相当する情報が書き込まれているため、カードに対してアクセスを行う端末が正当なものであるか否かを、カード側でも確認することも必要となる。この両方の確認、すなわち、カード認証（前者）、端末認証（後者）を行うのが相互認証である。

【０００３】相互認証において、端末及びカードのそれぞれに如何なる秘密鍵を持たせるか等は各種の形態があるが、その一つは、カード側に端末認証キー及びカード認証キー及び認証アルゴズム、さらに乱数生成アルゴリズム等を持たせ、セキュリティ上の観点から端末・カード間ではこれらのキー及びアルゴリズムの伝送を行わずに、端末側では相互認証に必要なキー及びアルゴリズムを独自に備える形態がある。例えば、端末には、マスターキーと個別化キー生成アルゴリズムとを持たせ、これに認証の都度カードから取得したカードＩＤとを用いて、ワークキーとして端末認証キー及びカード認証キーを生成する。また、端末側にもカードが所有しているのと同一の認証アルゴリズムを持たせておき、端末は上記で得た認証キーとこの認証アルゴリズムとを用いて（さらに、カード認証の場合には、端末が備えた乱数生成アルゴリズムも用いる。）、認証を行う形態である。

2

【０００４】ところが、端末において、これら①マスターキー、②個別化キー生成アルゴリズム、及び③認証アルゴリズムの、従来の格納方法としは、アルゴリズム②及び③は端末制御用プログラムに組み込んでおく形態、マスターキー①は制御用プログラムから任意にアクセス可能な端末のメモリに書き込んでおく形態等が採られていた。

【０００５】

【発明が解決しようとする課題】ところが、マスターキー等が任意にアクセス可能なメモリ中に格納されていると、端末制御のプログラムを知っている者によって読み出されてしまう恐れがあるという問題点があった。また、このマスターキーやアルゴリズムは、カードシステムを運営するユーザ毎、或いはシステム毎に変える必要があり、システムの製造者として多くのユーザーに対応するためには、各々異なる端末制御用プログラムを製作して組み込むことが必要となるという問題点があった。また、この他、システム運用後にマスターキーやアルゴリズムを変更する必要が生じた場合に、端末そのものを変更しなければならないという問題点もあった。

【０００６】

【課題を解決するための手段】そこで上記課題を解決する為に、本発明の情報記憶媒体の相互認証システムでは、端末側に独自に格納しておく、マスターキー、並びに、個別化キー生成アルゴリズム及び認証アルゴリズムを、セキュリティモジュールという端末本体とは別のモジュール、例えばＩＣカードに格納する形態とし、しかもこのセキュリティモジュールは少なくともマスターキーは書込むことが可能なマイクロコンピュータを用いて構成した。格納されたこれらの内容は外部から読出不可能な状態で格納しておき、また個別化キー生成アルゴリズムで生成したワークキーである端末認証キーやカード認証キーはセキュリティモジュール外部に出さずに該モジュール内のみで使用し、端末本体側ではこれらを用いた演算結果をセキュリティモジュールから取得する様にして相互認証に利用する構成とする。この結果、マスターキーやアルゴリズムが外部から不正に解読されて悪用されることなく、高いセキュリティ性を保つことができる。また、汎用的に同一の制御プログラムを有する端末本体を製造しておき、ユーザやシステムに応じたマスタ

ーキーと個別化キー生成及び認証の為のアルゴリズムが格納されたセキュリティモジュールを端末本体に組み込むことにより端末とするために、効率的にユーザー毎やシステム毎のマスターキーとアルゴリズムを管理できることとなる。

【０００７】

【発明の実施の形態】以下、図面を参照しながら本発明の情報記憶媒体の相互認証システムを説明する。本発明のシステムは情報記憶媒体としてＩＣカードと端末との関係に限定されるシステムではないが、ここでは、ＩＣカードと端末との相互認証を想定して以下説明する。図１は本発明の相互認証システムにおける、図２は従来の相互認証システムにおける、端末が保有する、マスターキー及びアルゴリズムの格納状態を対比した概念図である。図１及び図２においては、「Ａ」はマスターキーＡを、「Ｂ」はマスターキーＢを表し、また、アルゴリズムとしてｆは関数ｆを、ｇは関数ｇを表す。先ず、図１に示す本発明の情報記憶媒体の相互認証システムでは、端末本体１としては、ユーザが異なるシステムに対しても、全て同一の端末本体を用いることができる。この共通の端末本体１に対して、システムＡに用いるセキュリティモジュール２にはマスターキーＡ及び関数ｆが格納されているものを、システムＢに用いるセキュリティモジュール２ａにはマスターキーＢ及び関数ｇが格納されているものを用いる。そして、前記共通の端末本体に上記各システムで異なるセキュリティモジュールを組み込むことによって、システムＡ、システムＢ用のそれぞれの端末１０及び１０ａを構成することができる。

【０００８】次に、図２は従来の情報記憶媒体の相互認証システムにおける端末の一例を示す概念図であり、セキュリティモジュールを備えておらず、マスターキーや関数等は、システムＡ及びシステムＢ用のそれぞれの端末１０ｂ及び１０ｃとは分離独立可能な形態ではなく、端末１０ｂ、１０ｃと不可分の関係で端末に組み込まれている。端末１０ｂ、１０ｃに備える制御プログラムに、個別キー生成アルゴリズム及び認証アルゴリズムが組み込まれ、また端末が備えるメモリにマスターキーが格納されている。システムＡにおける端末１０ｂには、マスターキーＡ及びシステムＡ用の関数（図示せず）、同様にシステムＢにはマスターキーＢ及びシステムＢ用の関数（図示せず）が格納されて、端末１０ｃとなる。なお、図では便宜上、各システムは、一つのマスターキーＡ又はＢと、一つの関数ｆ又はｇとを備えているかの如く表現されているが、本発明のシステムでは、マスターキーは一つとは限らず、端末認証キー生成用とカード認証キー生成用とでそれぞれ独立の異なるマスターキーを備えている場合も意味する。また、関数、すなわちアルゴリズムは、個別キー生成アルゴリズム及び認証アルゴリズムの両方を備えていることを意味する。また、個別化キー生成アルゴリズムは、端末認証キー及びカード（情報記憶媒体）認証キー生成で共通の同一のもの、或いは別個のものでも良い。

【０００９】このように本発明の情報記憶媒体の相互認証システムは、従来の相互認証システムに対して、少なくともマスターキー、認証キー生成アルゴリズム及び認証アルゴリズムをモジュール化して、その他の部分を端末本体１として、端末本体１とセキュリティモジュール２とから端末１０を構成し、しかもセキュリティモジュールに格納したマスターキーやアルゴリズムは、該モジュールの外部からは読み取ることができない様にしたものである。

【００１０】そして、マスターキー並びに個別化キー生成アルゴリズム及び認証アルゴリズムは、セキュリティモジュールに読出不可能な状態で格納される。マスターキーは、セキュリティモジュールが備えるメモリに格納するが、これは例えばセキュリティモジュールをマイクロコンピュータを用いて構成することで、前記マスターキーを格納するメモリを該マイクロコンピュータの制御下に置き、マスターキーへのアクセスの属性を読出禁止属性とすることで達成される。このマスターキーについてはさらに書込は可能な属性としておけば、システム運用後にマスターキー変更の必要性が生じた場合に、セキュリティモジュールを使い捨てにせずにマスターキーを容易に変更することもできる。或いは、不正に書き換えられない様に、一旦マスターキーの書込を行ったならば、ファイル属性で或いは物理的に書込禁止にしておいても良い。また、個別化キー生成アルゴリズムや認証アルゴリズムは、このマイクロコンピュータの実行プログラムとして前記メモリ等に読出禁止属性を付けて書込んで置いても良いし、また、各アルゴリズム専用の演算回路（算術論理ユニット：ＡＬＵ）として組み込んでも良い。また、認証に用いる乱数を得る為の、乱数発生アルゴリズムの格納も行う場合は、マイクロコンピュータの実行プログラムとして組み込んでも良いし、或いは演算回路として組み込んでもよい。なお、マスターキーを格納するメモリはＣＰＵと共に１チップ化したメモリ、或いは別チップのメモリでも良い。また、上記の演算回路もＣＰＵ、メモリ等とともに１チップ化したマイクロコンピュータを用いても良い。

【００１１】上記の様な、セキュリティモジュールの物理的形態は、例えばＩＣカード等のカード状の形態、或いは携帯電話の一部で実用化されているＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）等のＩＣチップ等の形態である。カードとすることで、端末本体とは容易に分離独立させて、端末とは別のセキュリティ性の管理された所で、セキュリティモジュールにマスターキーの設定を行ったり、各ユーザ毎の或いは各システム毎のセキュリティモジュールの製造、或いは設定の変更を安全に行えることが可能となる。この様にカード形態の場合、容易に端末本体への組込み及び脱着が

できるが、本発明のセキュリティモジュールはカード以外の形態でも良い。セキュリティモジュールの上記機能は、１チップ或いは数チップのＩＣによって実現できるので、これらを１パッケージとしてまとめたＩＣとしても良く、端末本体のＩＣソケットに実装することで、セキュリティモジュールを端末本体から脱着可能に組み込むことができる。なお、本発明では、セキュリティモジュールは必ずしも脱着可能に分立独立できる形態で端末本体に組み込むことは必要ではない。

【００１２】次に、上記セキュリティモジュールに読出不可能な状態で内蔵されている、マスターキー並びに個別化キー生成アルゴリズム及び認証アルゴリズム、さらに適宜乱数発生アルゴリズムは、それらを該モジュールから解読されることなく、それらを用いた演算結果のみが端末本体側に読み出されて認証に使用される。端末はカードＩＤ（情報記憶媒体の識別情報）をカードから取得し、これとマスターキーと個別化キー生成アルゴリズムを用いて、カードが保有する端末認証キーやカード認証キーを生成するが、さらに、セキュリティモジュールのマイクロコンピュータにより、この各認証キーもセキュリティモジュールから読み出されることなく該モジュール内で使用してその使用結果のみを端末本体側では読み出すことが出来る様にすれば、ワークキーである認証キーに対するセキュリティ性も向上する。

【００１３】そして、以上のようなセキュリティモジュールを備えた端末を用いる、本発明の情報記憶媒体の相互認証システムのシステム全体としては、情報記憶媒体には従来公知の相互認証機能を有するＩＣカード等が使用でき、通常は複数の端末がホストコンピュータに接続されたシステムとして構成される。相互認証機能を有するＩＣカードは、ＩＣメモリ以外にＣＰＵ等を備えたマイクロコンピュータ等を備えることで相互認証機能を実行する。なお、ＩＣメモリ以外に光メモリ等の光学記録メモリ、磁気メモリ等を備えていても良い。また、情報記憶媒体のＩＣカードがプリペイドＩＣカードであれば、プリペイドＩＣカードシステムとなり、情報記憶媒体をＩＣカードとすれば、その使い方によって各種用途に適した、相互認証機能を有するＩＣカードシステムとなる。

【００１４】

【実施例】次に、本発明の情報記憶媒体の相互認証システムの一実施例としてＩＣカードシステムを説明する。図３は本システムの一実施例における端末１０について、そのセキュリティモジュール２の概略構成図である。同図のシステムの端末１０は、従来の相互認証システム機能を有するＩＣカードシステムの端末において、少なくともマスターキー、認証キー生成アルゴリズム及び認証アルゴリズムを、ＩＣカード形態のモジュールとして、その他の部分を端末本体１として、端末本体１とセキュリティモジュール２とから端末１０を構成し、しかもセキュリティモジュールに格納したマスターキーや各アルゴリズム、さらに得られる認証キーも、該モジュールの外部からは読み取ることができない様に、マイクロコンピュータで制御したものである。また、システム全体としては、情報記憶媒体はＩＣメモリとＣＰＵを内蔵し相互認証機能を有するＩＣカードを使用し、通常は複数の端末がホストコンピュータに接続されたシステムとして構成される。なお、このＩＣカードをプリペイドＩＣカードとすれば、プリペイドＩＣカードシステムとなる。

【００１５】図３に示すセキュリティモジュール２は、マイクロコンピュータ３と、個別化キー生成アルゴリズム及び認証アルゴリズムをおのおの演算する暗号回路６、認証に用いる乱数を発生する乱数発生アルゴリズムを演算する乱数発生回路７とを備える。また、マイクロコンピュータ（ＭＰＵ）３は、中央演算処理装置であるＣＰＵ４とメモリ５とが１チップのＬＳＩとなっており、メモリ５にはＣＰＵが実行する各種プログラム、マスターキー等が格納され、また作業用メモリもこの中に確保されている。同図の様にメモリへのアクセスはＣＰＵを通してアクセス可能であり、マスターキーは、例えば読出禁止属性を有するファイル等としての形態で、外部から読出不可能な状態で、セキュリティモジュールに格納されている。また、マスターキー及び個別化キー生成アルゴリズムを用いて生成される端末認証キー及びカード認証キーの認証キーは、セキュリティモジュール内でのみ使用される。

【００１６】そして、メモリ５に端末認証用として（後述する）マスターキーＡ１を、カード認証用としてマスターキーＡ２が格納され、暗号回路６は、端末認証キー及びカード認証キーの生成に用いる個別化キー生成アルゴリズムとして関数ｇを、認証アルゴリズムとして関数ｆを演算し、乱数発生回路７は、（後述する）乱数（関数）Ｂを演算し、そして、マイクロコンピュータ３はこれらを用いて、認証の為の照合用データを作成し、端末本体側へ返す。

【００１７】次に、図４の端末認証、図５のカード認証のフロー図を参照しながら本発明の情報記憶媒体の相互認証システムによる認証のフローを説明する。

【００１８】図４で、左側はＩＣカード側の処理を、右側は端末内のセキュリティモジュール内の処理を示す。端末本体（以下、単に端末）は認証に必要なＩＣカードとセキュリティモジュールとのデータの受渡しを行う。ＩＣカードが端末を認証する端末認証のフローでは、先ず、端末はＩＣカードから端末認証用の「カードＩＤ１」を読み取り、これを端末内のセキュリティモジュールに渡す（ステップＳ１、以下Ｓ１等と記す）。そして、セキュリティモジュールでは上記「カードＩＤ１」と該モジュールに格納された「マスターキーＡ１」とから個別化キー生成アルゴリズムである関数ｇを用いて、

端末認証用のワークキーである「認証キー１ｇ（ＩＤ１）」を生成する（Ｓ２）。次に、端末はＩＣカードの乱数（関数）Ａで発生させた「乱数ＲＮＡ」を読み取りセキュリティモジュールに渡す（Ｓ３）。そして、セキュリティモジュールは、前記生成済みの「認証キー１ｇ（ＩＤ１）と上記「乱数ＲＮＡ」とから認証アルゴリズムである関数ｆを用いて「照合用データｆ（ｇ（ＩＤ１）、ＲＮＡ）」生成する（Ｓ４）。次に、端末はセキュリティモジュールで生成済みの「照合用データｆ（ｇ（ＩＤ１）、ＲＮＡ）」をＩＣカードに伝送する（Ｓ５）。一方、ＩＣカード側では、上記「照合用データｆ（ｇ（ＩＤ１）、ＲＮＡ）」がＩＣカード内で生成する照合用データと同一であるかを比較するための以下の処理を行う。ＩＣカードは、ＩＣカードの乱数（関数）Ａで発生させ前記で端末に伝送したものと同一の「乱数ＲＮＡ」と、ＩＣカード内に格納されている端末認証用の「認証キー１（ｇ（ＩＤ１）」とから（ＩＣカードに格納されている）関数ｆを用いて、「照合用データｆ（ｇ（ＩＤ１）、ＲＮＡ）」生成する（Ｓ６）。そして、ＩＣカードのこの自己生成した照合用データと、端末側で生成した照合用データとを比較する（Ｓ７）。一致している場合はＩＣカードは端末を正しいものと認証とする。

【００１９】次は、図５で、端末がＩＣカードを認証するカード認証のフローを説明する。先ず、端末はＩＣカードからカード認証用の「カードＩＤ２」を読み取り、これを端末内のセキュリティモジュールを渡す（ステップＳ１１）。そして、セキュリティモジュールでは上記「カードＩＤ２」と該モジュールに格納されたカード認証用のマスターキーである「マスターキーＡ２」とから関数ｇを用いて、カード認証用の「認証キー２ｇ（ＩＤ２）」を生成する（Ｓ１２）。次に、端末はセキュリティモジュールに格納された乱数（関数）Ｂで発生させた「乱数ＲＮＢ」をＩＣカードに伝送する。そして、ＩＣカードは自己が保有する「認証キー２ｇ（ＩＤ２）と上記「乱数ＲＮＢ」とから（自己が保有する）関数ｆを用いて「照合用データｆ（ｇ（ＩＤ２）、ＲＮＢ）」生成する（Ｓ１４）。次に、端末はこの「照合用データｆ（ｇ（ＩＤ２）、ＲＮＢ）」をＩＣカードから読み出し、セキュリティモジュールに渡す（Ｓ１５）。また、端末側では、上記「照合用データｆ（ｇ（ＩＤ２）、ＲＮＢ）」が端末内で生成する照合用データと同一であるかを比較するための以下の処理を行う。端末のセキュリティモジュールは、その乱数（関数）Ｂで発生させ前記でＩＣカードに伝送したのと同一の「乱数ＲＮＢ」と、前記ステップＳ１２で生成した「認証キー２（ｇ（ＩＤ２）」とから（セキュリティモジュールに格納されている）関数ｆを用いて、「照合用データｆ（ｇ（ＩＤ２）、ＲＮＢ）」生成する（Ｓ６）。そして、セキュリティモジュールはこの自己生成した照合用データと、ＩＣカード側で生成した照合用データとを比較する（Ｓ１７）。一致している場合は端末はＩＣカードを正しいものと認証とする。以上の様にして、端末認証及びカード認証が行われる。

【００２０】なお、本発明の情報記憶媒体の相互認証システムは、上記実施例に限定されず、前述の如く各種形態があり得る。例えば、上記実施例の相互認証では、端末認証キー及びカード認証キーの生成に異なるカードＩＤを用いたが、各認証キーで同一のカードＩＤを用いる等である。また、情報記憶媒体としてのＩＣカードは、その用途により、クレジットカード、バンクカード、プリペイドカード等の多様である。

【００２１】

【発明の効果】端末が相互認証の演算に必要とする、マスターキー及びアルゴリズムがセキュリティモジュール内に格納され、その演算と演算の途中結果を外部から読み出すことが不可能であり、キーやアルゴリズムを盗み出すことができず、セキュリティ性に優れる。セキュリティモジュールに格納するマスターキーを、マイクロコンピュータによって読出不可能且つ書込可能に制御されたメモリに格納することで、マスターキーはセキュリティ性を保った上で、マスターキーの途中での変更もできる。また、マスターキーやこれらアルゴリズムを、端末本体と切り離した状態でセキュリティモジュールで設定ができるため、ユーザー毎やシステム毎の管理が行い易い。また、マスターキーやこれらアルゴリズムを、変更する必要が生じた場合に、セキュリティモジュールのみを交換するだけで、容易に変更ができる。

【図面の簡単な説明】

【図１】本発明の情報記憶媒体の相互認証システムにおける端末の概念図。

【図２】従来の情報記憶媒体の相互認証システムにおける端末の概念図。

【図３】本発明の相互認証システムの一実施例であるＩＣカードシステムでの端末のセキュリティモジュールを中心にした概略構成図。

【図４】本発明における端末認証処理の一例を示すフロー図。

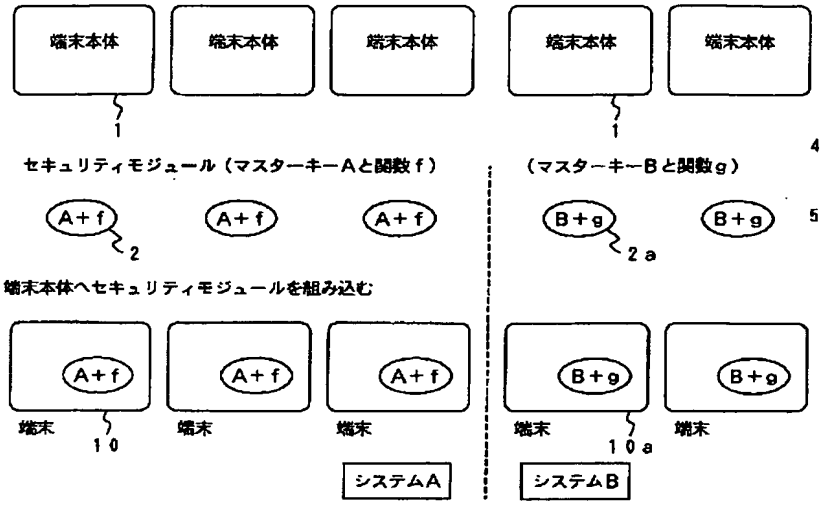
【図５】本発明におけるカード認証処理の一例を示すフロー図。

【符号の説明】

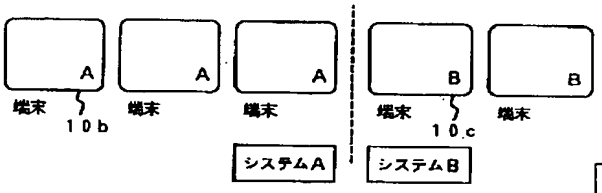
１　端末本体
２、２ａ　セキュリティモジュール
３　ＭＰＵ
４　ＣＰＵ
５　メモリ
６　暗号回路
７　乱数発生回路
１０、１０ａ～１０ｃ　端末
Ａ、Ａ１、Ａ２、Ｂ、Ｂ１、Ｂ２　マスターキー

ｆ、ｇ　関数、アルゴリズム

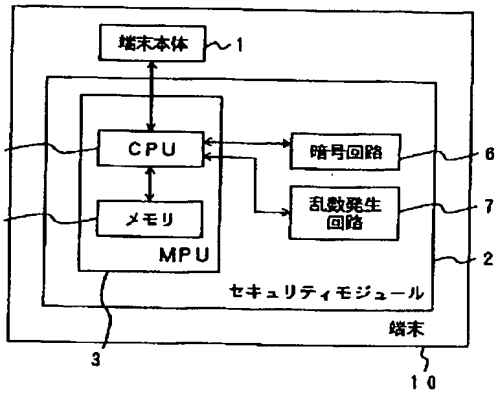
【図１】



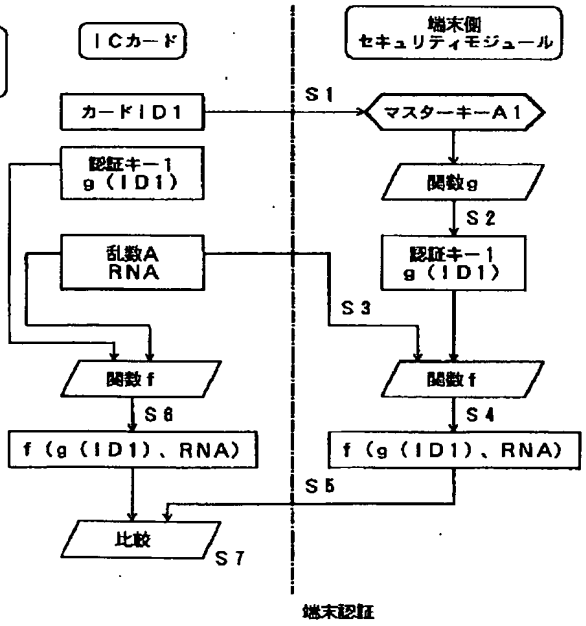
【図２】



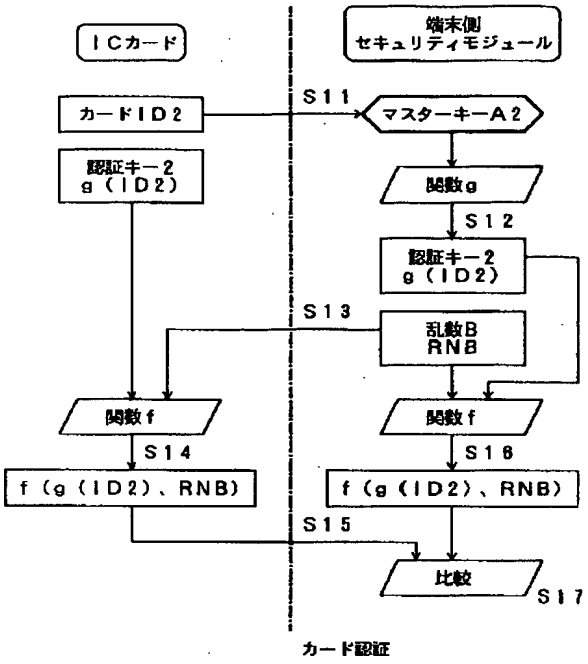
【図３】



【図４】



【図５】



フロントページの続き

(51) Int. Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ　9/00	６０１Ａ	
	9/10				６２１Ａ	
	9/32				６７５Ａ	